

# Introduction

---

Part I of this handbook surveys critical information infrastructure protection (CIIP) efforts in fourteen countries, namely Australia, Austria, Canada, Finland, France, Germany, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

For each survey, four focal points of high importance covering conceptual and organizational aspects of CIIP are considered:

## *(1) Critical Sectors*

The first section lists the critical sectors identified by the specific country and provides, when available, definitions of CII and CIIP.

## *(2) Initiatives and Policy*

The second section gives an overview of the most important steps taken at the governmental level since the late 1990s to handle CIIP. The focus is on initiatives and the main elements of CIIP policy. This includes descriptions of specific committees, commissions, task forces, and working groups, main findings of key official reports and fundamental studies, and important national programs.

## *(3) Organizational Overview*

The third section gives an overview of important public actors in the national CIIP organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are omitted. Due to the growing importance of public private partnerships, the most important of these are presented.

## *(4) Early Warning Approaches*

The fourth section describes national organizations responsible for CIIP early warning, namely CIIP-related information-sharing organizations such as *CERTs* (Computer Emergency Response Teams), *ISACs* (Information Sharing and Analysis Centers), etc. Furthermore, reference is made to plans for the development of comprehensive early warning alert and incident report structures.

The key question underlying Part I is: *What national approaches to critical information infrastructure protection exist?*

The surveys were compiled in a three-step procedure.

- 1) First, open-source material was collected from online resources, publicly available government papers, workshops, and conference proceedings. This information was used to write a first draft of the country surveys. However, the availability of this open-source information, and especially the availability of documents on the Internet, varies considerably in quantity and quality from country to country. Additionally, a lot of relevant information is only available in the original language.
- 2) The second and most important step was the collaboration with the national experts from government and government-related organizations in the field. Whenever possible, at least two experts per country were consulted for reviews. The experts were asked to correct, complete, and update the draft country surveys.
- 3) Finally, all of the national experts' input was worked into the final version of the country studies.

Since expert input was crucial for all country surveys, it is obvious that the individual perspectives and viewpoints of the consulted experts had a significant impact on the end result. This is also one of the major reasons why the individual surveys differ considerably in focus and general direction, and in their understanding of the nature of CIIP.

Center for Security Studies, ETH Zurich  
Volume 2, Zürich 2004.

**The International CIIP Handbook 2004:  
An Inventory and Analysis of Protection Policies in Fourteen  
Countries**

Myriam Dunn and Isabelle Wigert

edited by  
Andreas Wenger and Jan Metzger

Online version provided by the  
International Relations and Security Network

A public service run by the  
Center for Security Studies at the ETH Zurich  
© 1996-2004

